(a) From subsection (c)(3) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of the investigation, and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process.

(b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation, to the existence of the investigation, and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an impossible administrative burden by requiring investigations to be continuously reinvestigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of Federal law, the accuracy of information obtained or introduced occasionally may be unclear or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsections (e)(4)(G), (e)(4)(H), and (e)(4)(I) (Agency Requirements), and (f) (Agency Rules) because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

[71 FR 20523, Apr. 21, 2006]

EDITORIAL NOTE: For FEDERAL REGISTER citations affecting appendix C to part 5, see the List of CFR Sections Affected, which appears in the Finding Aids section of the printed volume and on GPO Access.

PART 7—CLASSIFIED NATIONAL SECURITY INFORMATION

Sec.

AUTHORITY: 5 U.S.C. 301; Pub. L. 107–296, 116 Stat. 2135 (6 U.S.C. 101); E.O. 12958, 60 FR 19825, 3 CFR, 1995 Comp., p. 333; E.O. 13142, 64 FR 66089, 3 CFR, 1999 Comp., p. 236; 32 CFR part 2001.

SOURCE: 70 FR 61213, Oct. 21, 2005, unless otherwise noted.

§ 7.1 Purpose.

The purpose of this part is to ensure that information within the Department of Homeland Security (DHS) relating to the national security is classified, safeguarded, and declassified pursuant to the provisions of Executive Order 12958, as amended, and implementing directives from the Information Security Oversight Office (ISOO)

of the National Archives and Records Administration (NARA).

§ 7.2 Scope.

(a) This part applies to all employees, detailees and non-contractor personnel outside the Executive Branch who are granted access to classified information by the DHS, in accordance with the standards in Executive Order 12958, as amended, and its implementing directives.

(b) This part does not apply to contractors, grantees and other categories of personnel falling under the purview of Executive Order 12829, National Industrial Security Program, and its implementing directives.

(c) This part is independent of and does not affect any classification procedures or requirements of the Atomic Energy Act of 1954, as amended (42 U.S.C. 2011 *et seq*).

(d) This part does not, and is not intended to, create any right to judicial review, or any other right or benefit or trust responsibility, substantive or procedural, enforceable by a party against the United States, its agencies or instrumentalities, its officers or employees, or any other person. This part creates limited rights to administrative review of decisions. This part does not, and is not intended to, create any right to judicial review of administrative action.

§ 7.3 Definitions.

The terms defined or used in Executive Order 12958, as amended, and the implementing directives in 32 CFR parts 2001 and 2004, are applicable to this part.

Subpart A—Administration

§ 7.10 Authority of the Chief Security Officer, Office of Security.

(a) The DHS Chief Security Officer (hereafter ''Chief Security Officer'') is designated as the Senior Agency Official as required by section 5.4(d) of Executive Order 12958, as amended, and, except as specifically provided elsewhere in this part, is authorized to administer the DHS Classified National Security Information program pursuant to Executive Order 12958, as amended.

(b) The Chief Security Officer shall, among other actions:

(1) Oversee and administer the DHS's program established under Executive Order 12958, as amended;

(2) Promulgate implementing regulations;

(3) Establish and maintain Department-wide security education and training programs;

(4) Establish and maintain an ongoing self-inspection program including the periodic review and assessment of the DHS's classified product;

(5) Establish procedures to prevent unnecessary access to classified information, including procedures that:

(i) Require that a need for access to classified information is established before initiating administrative procedures to grant access; and

(ii) Ensure that the number of persons granted access to classified information is limited to the minimum necessary for operational and security requirements and needs;

(6) Develop special contingency plans for the safeguarding of classified information used in or near hostile or potentially hostile areas;

(7) Coordinate with the DHS Chief Human Capital Officer, as appropriate to ensure that the performance contract or other system used to rate personnel performance includes the management of classified information as a critical element or item to be evaluated in the rating of:

(i) Original classification authorities;

(ii) Security managers or security specialists; and

(iii) All other personnel whose duties significantly involve the creation or handling of classified information;

(8) Account for the costs associated with implementing this part and report the cost to the Director of ISOO;

(9) Assign in a prompt manner personnel to respond to any request, appeal, challenge, complaint, or suggestion concerning Executive Order 12958, as amended, that pertains to classified information that originated in a DHS component that no longer exists and for which there is no clear successor in function;

(10) Report violations, take corrective measures and assess appropriate sanctions as warranted, in accordance